New DES based on elliptic curves

Ghada Abdelmouez M. Abdelhady*
Basic Science Dept.
German University in Cairo (GUC)
New Cairo city
Main Entrance Eltagamoa Elkhames, 0125871028
Egypt

Fathy S. Helail†
Basic Science Dept.
German University in Cairo (GUC)
Egypt

Abdellatif A. Elkouny§
Air Defense Research and Development Center
Egyptian Army
Egypt

Abstract

It is known that symmetric encryption algorithms are fast and easy to implement in hardware. Also elliptic curves have proved to be a good choice for building encryption system. Although most of the symmetric systems have been broken, we can create a hybrid system that has the same properties of the symmetric encryption systems and in the same time, it has the strength of elliptic curves in encryption. As DES algorithm is considered the core of all successive symmetric encryption systems, we modified DES using elliptic curves and built a new DES algorithm that is hard to be broken and will be the core for all other symmetric systems.

Keywords: *DES, Elliptic Curves, symmetric encryption, hybrid system.*